

1 **CLAIMS**

- 2
- 3 1. A method for providing cryptographic keys usable in a network of connected
- 4 computer nodes applying a signature scheme, the method executable by a first
- 5 computer node comprising the steps of:
- 6
- 7 - generating a random secret key;
- 8
- 9 - generating an exponent interval having a first random limit, wherein, with a
- 10 probability close to certainty, each element of the exponent interval has a unique
- 11 prime factor that is larger than a given security parameter;
- 12 - providing a public key comprising an exponent-interval description and a public
- 13 key value derived from the random secret key, such that the random secret key and a
- 14 selected exponent value from the exponent interval are usable for deriving a
- 15 signature value on a message to be sent within the network to a second computer
- 16 node for verification.
- 17
- 18 2. The method according to claim 1, wherein the step of generating a random secret key
- 19 comprises using two primes, the product of which is part of the public key.
- 20
- 21 3. The method according to claim 1, wherein the step of generating a random secret key
- 22 comprises selecting an integer value defining a class group and selecting two
- 23 elements of the class group.
- 24
- 25 4. The method according to claim 3, wherein the step of providing a public key
- 26 comprises computing a modified public key value under use of the selected two
- 27 elements and the exponent interval.
- 28

- 1 5. A method for providing a signature value on a message in a network of connected
2 computer nodes, the method executable by a first computer node comprising the
3 steps of:
4
5 - selecting an exponent value from an exponent interval, wherein each element of the
6 exponent interval has, with a probability close to certainty, a unique prime factor that
7 is larger than a given security parameter; and
8
9 - deriving the signature value from a provided secret key, the selected exponent
10 value, and the message, the signature value being sendable within the network to a
11 second computer node for verification.
12
13 6. The method according to claim 5, wherein the step of deriving the signature value
14 further comprises a computation of the i -th root of a value derived from the message
15 and the secret key using a cryptographic hash function, the i being the exponent
16 value.
17
18 7. A method for verifying a signature value on a message in a network of connected
19 computer nodes, the method executable by a second computer node comprising the
20 steps of:
21
22 - receiving the signature value from a first computer node; and
23 - verifying whether an exponent value is contained in an exponent interval, wherein
24 each element of the exponent interval has, with a probability close to certainty, a
25 unique prime factor that is larger than a given security parameter, the signature value
26 is invalid if the exponent value is not contained in the exponent interval.
27

- 1 8. The method according to claim 7, wherein the step of verifying further comprises a
2 computing step of raising a computed signature root value that being part of the
3 signature value to the power of the exponent value.
4
- 5 9. An apparatus to provide a signature value on a message in a network of connected
6 computer nodes, the apparatus executable by a first computer node comprising:
7
- 8 - means for selecting an exponent value from an exponent interval, wherein each
9 element of the exponent interval has, with a probability close to certainty, a unique
10 prime factor that is larger than a given security parameter; and
11
- 12 - means for deriving the signature value from a provided secret key, the selected
13 exponent value, and the message, the signature value being sendable within the
14 network to a second computer node for verification.
15
- 16 10. An apparatus to verify a signature value on a message in a network of connected
17 computer nodes, the apparatus executable by a second computer node comprising:
18
- 19 - means for receiving the signature value from a first computer node; and
20
- 21 - means for verifying whether an exponent value is contained in an exponent interval,
22 wherein each element of the exponent interval has, with a probability close to
23 certainty, a unique prime factor that is larger than a given security parameter , the
24 signature value is invalid if the exponent value is not contained in the exponent
25 interval.
26
- 27 11. A computer device comprising:
28
- 29 a computer program product according to claim 9; and

1
2 a processor for executing the computer program product when the computer program
3 product is run on the computer device.
4

5 12. An apparatus to provide cryptographic keys usable in a network of connected
6 computer nodes applying a signature scheme, the apparatus executable by a first
7 computer node comprising:
8

9 - means for generating a random secret key;
10

11 - means for generating an exponent interval having a first random limit, wherein,
12 with a probability close to certainty, each element of the exponent interval has a
13 unique prime factor that is larger than a given security parameter; and
14

15 - means for providing a public key comprising an exponent-interval description and a
16 public key value derived from the random secret key, such that the random secret key
17 and a selected exponent value from the exponent interval are usable for deriving a
18 signature value on a message to be sent within the network to a second computer
19 node for verification.
20

21 13. An article of manufacture comprising a computer usable medium having computer
22 readable program code means embodied therein for causing provision of cryptographic
23 keys usable in a network of connected computer nodes applying a signature scheme, the
24 computer readable program code means in said article of manufacture comprising
25 computer readable program code means for causing a computer to effect the steps of
26 claim 1.

27 14. A program storage device readable by machine, tangibly embodying a program of
28 instructions executable by the machine to perform method steps for providing

1 cryptographic keys usable in a network of connected computer nodes applying a signature
2 scheme, said method steps comprising the steps of claim 1.

3 15. An article of manufacture comprising a computer usable medium having computer
4 readable program code means embodied therein for causing provision of a signature value
5 on a message in a network of connected computer nodes, the computer readable program
6 code means in said article of manufacture comprising computer readable program code
7 means for causing a computer to effect the steps of claim 5.

8 16. A program storage device readable by machine, tangibly embodying a program of
9 instructions executable by the machine to perform method steps for providing a signature
10 value on a message in a network of connected computer nodes, said method steps
11 comprising the steps of claim 5.

12 17. An article of manufacture comprising a computer usable medium having computer
13 readable program code means embodied therein for causing provision of a signature value
14 on a message in a network of connected computer nodes, the computer readable program
15 code means in said article of manufacture comprising computer readable program code
16 means for causing a computer to effect the steps of claim 7.

17 18. A program storage device readable by machine, tangibly embodying a program of
18 instructions executable by the machine to perform method steps for providing a signature
19 value on a message in a network of connected computer nodes, said method steps
20 comprising the steps of claim 7.

21 19. A computer program product comprising a computer usable medium having
22 computer readable program code means embodied therein for causing provision of a
23 signature value on a message in a network of connected computer nodes, the computer

1 readable program code means in said computer program product comprising computer
2 readable program code means for causing a computer to effect the functions of claim 9.

3 20. A computer program product comprising a computer usable medium having
4 computer readable program code means embodied therein for causing verification of a
5 signature value on a message in a network of connected computer nodes, the computer
6 readable program code means in said computer program product comprising computer
7 readable program code means for causing a computer to effect the functions of claim 10.

8 21. A computer program product comprising a computer usable medium having
9 computer readable program code means embodied therein for causing provision of
10 cryptographic keys usable in a network of connected computer nodes applying a signature
11 scheme, the computer readable program code means in said computer program product
12 comprising computer readable program code means for causing a computer to effect the
13 functions of claim 12.